FORSVARSDEPARTEMENTET
SAKNR.: 10/ 00794 -16
28 JUN 2010
ARKBET: 206
KASSERES 5 ÅR
KASSERES 30 ÅR
REVARES

Det Kongelige Forsvarsdepartement

Postboks 8126 Dep

0032 Oslo

Att.: Ole Felix Dahl

Deres/Your ref.: Vår/Our ref.: UU190/10PAE Trondheim, 25.06.2010

FORSLAG TIL STRATEGI FOR CYBERSIKKERHET – KOMMENTARER FRA UNINETT-KONSERNET

Det vises til høringsbrev om forslag til nasjonal strategi for cybersikkerhet, datert 30.3.2010.

UNINETT-konsernet leverer nett og nettjenester til norske universiteter, høgskoler og forskningsinstitusjoner, og håndterer andre nasjonale IKT-oppgaver til beste for hele samfunnet. Konsernet eies av Kunnskapsdepartementet og består av morselskap og tre datterselskaper med rundt 100 faste ansatte. Vårt høringssvar inkluderer kommentarer fra datterselskapene UNINETT FAS, UNINETT Norid og UNINETT Sigma.

Generelt er UNINETT enig i intensjonen med å implementere en nasjonal strategi for cybersikkerhet. Utkastet til strategi gir en oversiktlig og utfyllende beskrivelse av sikkerhetssituasjonen og inneholder en god samling av tiltak.

Vi har imidlertid kommentarer til noen av de tiltakene som er foreslått.

Punkt 2.1

Avsnittet "Hvorfor?": I tillegg til å identifisere de *mest kritiske* IKT-systemene, kan det være interessant å stille spørsmålet: *Hva er minimum av funksjonalitet som samfunnet trenger for å fungere?* Jf. fotnote 32: Det finnes ikke noen klar definisjon av begrepet *kritisk infrastruktur.*

Tiltak 1,3,4,5:

Vi kunne ønske en mer konkret beskrivelse av hva disse tiltakene går ut på.

Tiltak 3:

Vi savner en beskrivelse av *hvordan* formidlingen av risikobildet kan forbedres.

UNINETT

Postadresse/Postal address
UNINETT AS
NO-7465 Trondheim

Besøksadresse/Visiting address
Abels gate 5
Trondheim, Norway

Foretaksnr./Company reg. no.: 968 100 211
Bankgiro/Bank account: 4200 40 67953

Epost/E-mail: info@uninett.no
Tel.: +47 73 55 79 00
Fax: +47 73 55 79 01

Punkt 2.2

Tiltak 6:

Det bør utarbeides en liste over sikkerhetsutstyr og -løsninger som er godkjent og/eller sertifisert. Denne listen må jevnlig revideres og oppdateres av f.eks. NSM eller lignende organ. Dette vil kunne bidra til at sikring av IKT-løsninger blir enklere og antakelig vesentlig bedre enn i dag. Ulempen er at slike ordninger fører til dyrere produkter. Offentlige og private aktører som innehar kritiske IKT-systemer bør likevel tilstrebe å benytte seg av slike produkter i størst mulig grad. Det er imidlertid en forutsetning at det samtidig etableres effektive og levende styringssystemer for informasjonssikkerhet, f.eks. som beskrevet i ISO 27001/27002. Uten at sistnevnte er på plass vil sertifiseringsordninger lett kunne bli en sovepute og kun føre til at produktene blir dyrere, uten at man oppnår ønsket sikkerhetsgevinst.

Det bør vurderes hvor i regelverket slike krav skal nedfelles. Noen av kravene vil være egnet som forskrift, andre som anbefalinger.

Tiltak 8:

Det burde kanskje vurderes om denne fremgangsmåten kan brukes også i andre sammenhenger, f.eks. for lagrede data og styringssystemer.

Punkt 2.3

Under "status" peker man blant annet på at sikkerhetsforståelsen hos eiere av systemer og infrastruktur er liten, og at det er manglende bevissthet i organisasjoner om hvordan organisasjonskultur og sikkerhetskultur påvirker holdninger, adferd og bruk av IKT-systemer. Videre stilles det spørsmål om dokumentert sikkerhetskompetanse hos driftspersonellet.

Det kan virke som om at de foreslåtte tiltakene (tiltak 11 og 12) primært retter seg mot å heve kompetansen hos driftspersonell og brukere. Dette mener vi er utilstrekkelig, fordi alt arbeid med informasjonssikkerhet først og fremst må forankres i virksomhetens ledelse. Erfaringen fra vår sektor er at denne forankringen har vært mangelfull, og vi har grunn til å tro at situasjonen ikke er vesentlig bedre i andre typer virksomheter. Tilstanden kan føre til at sikkerhetsnivået settes på et for lavt nivå i organisasjonen og at sikkerhetstiltakene dermed blir ubalanserte. Ledelsen og systemeierne må jevnlig gjøre seg kjent med hvilke risikoer som er knyttet til sine informasjonseiendeler og deretter gi føringer for hvilke beskyttelsestiltak som skal iverksettes i alle ledd av virksomheten. Dette kan oppnås ved at det utvikles styringssystemer for informasjonssikkerhet (ISO 27001/27002) og at dette blir en del av virksomhetens strategiprosess. Virksomhetens beskyttelsestiltak bør utformes slik at det kan gjennomføres tilsyn med hensyn til oppfyllelse av kravene, og det bør vurderes i hvilken grad beskyttelsestiltakene skal basere seg på regulatoriske krav.

Det bør derfor beskrives nye tiltak under dette kapitlet som ivaretar ovenstående kommentar.

Punkt 2.4

Tiltak 13:

Tredje setning "samfunnets samlede deteksjonskapabiliteter..." er etter vår oppfatning det som avsnittet dreier seg om og bør stå først.

En utvidelse av VDI slik det fremstår i dag er ikke optimalt fordi denne teknologien omfatter en for liten del av det totale trusselbildet.

Punkt 2.5

Tiltak 17:

Man bør ikke formulere tiltaket slik at det kan forstås som et partsinnlegg i diskusjonen om implementering av Datalagringsdirektivet. Generelt bør man være svært varsom med tiltak som legger opp til utvidet adgang til registrering og lagring av kommunikasjon. Vi viser til punkt 1.1 i strategiutkastet som bl.a. sier: "Sikkerhetstiltakene skal beskytte, ikke utfordre, grunnleggende rettigheter".

Punkt 2.6

Vi synes ikke det er godtgjort at det å etablere et nasjonalt cybersenter som beskrevet er et godt tiltak. Vi er skeptiske til en mulig sammenblanding av rollene myndighetsmakt og rådgivning.

Med hilsen

Per Arne Enstad

Sikkerhetskoordinator

UNINETT